M403 Modern Algbera - Comments

Aolong Li
aolli@iu.edu

1 Homework #6

2.45 In general groups (except the groups such as $(\mathbb{R}, \cdot)$, $(\mathbf{C}, \cdot)$), we don't have the definitions of " $\sqrt{g}$ " and " $g \geq 0$ ". Hence the proofs based on these conceptions do not make sense. Instead, consider the map

$$\begin{aligned} \varphi : G &\longrightarrow G \\ g &\mapsto g^2 \end{aligned}$$

Equivalently, you need to prove this map is injective. Here you may use the result appeared in the previous homework: If X and Y are finite sets with the same number of elements, the function (map) $f : X \to Y$ is injective if and only if f is surjective (Exercise 2.13).

2.46 Note that

$$G = \{e\} \cup \{g \in G : \mathrm{ord}(g) = 2\} \cup \{g \in G : \mathrm{ord}(g) > 2\}$$

2.47 Be careful about what the question asks. Do not miss the cases $n = 1, 2, \cdots, 9$.

And consider the product of several cycles (especially when $n = 10$), instead of thinking just one cycle or the product of two cycles.

Canvas Problems

- Remember to evaluate the third powers! (Be careful when you are reading!)
- Almost everyone did not explain why the length and the angle of the multiplicative inverse make sense. Try to think about the geometrical meaning of $z_1 \cdot z_2$ where z_1 and z_2 are complex numbers.

2 Homework #9

3.1(i) It is natural to disprove this by using the counterexample that $\pi \in S = \{r + s\pi;\ s, r \in \mathbb{Q}\}$ but $\pi^2 \notin S$. But the statement that π^2 can not be written in the form $r + s\pi$ is not obvious, in other words, needs some words to clarify this. (Hint: use the fact that π is transcendental, that is, π is not the root of the polynomial whose coefficients are rational numbers.)

3.2 We cannot conclude that $e = 1$ from $r(e - 1) = 0$. This only holds when R is a domain. Actually, this statement is readily to obtain. Consider the trick we use to prove there is only one identity in a group.

3.4 Someone show $a - b = b - a$ does not hold. However, this is called "commutativity". Instead, we need to disprove the 'associativity", i.e. $(a - b) - c \neq a - (b - c)$.

For (ii), to say a ring R, except that it has a well-known name (e.g. *zero ring* and *integer ring* $\mathbb{Z}$), we need to define (or explain) the *elements* of R and its *two operations*.

So $\{0\}$ is not a ring and $(\{0\}, +, \cdot)$ is a ring (or just simply say the zero ring).

3.8 Note there are several equivalent criteria for the domain:

- An integral domain is commutative ring R with $1 \neq 0$ satisfies cancellation law.
- An nonzero (i.e. $1 \neq 0$) commutative ring R is an integral domain $\iff$ the product of any non-zero elements of R is nonzero.
- An nonzero (i.e. $1 \neq 0$) commutative ring R is an integral domain $\iff$ if $r, s \in R$ and $r \cdot s = 0$, then $r = 0$ or $s = 0$.

3.11 Note that $z_1 \cdot z_2 = 0 \Longleftrightarrow |z_1| \cdot |z_2| = 0 \Longleftrightarrow |z_1| = 0$ or $|z_2| = 0$.

3.15 From the definition, if R is a domain, it has to be a commutative ring. This is the main difference between (ii) and (iii).

3 Homework #10

3.17(ii) Note that $\mathbb{Z}/p\mathbb{Z}$ is always a field when p is a prime and it is well known that primes numbers are infinite, in other words, we can have a prime number as large as possible.

3.17(vii) To generate the $\mathrm{Frac}(R)$ form a ring R can be regarded as a procedure to extend a ring to a domain as small as possible. So an alternative definition of $\mathrm{Frac}(R)$ is the *smallest* domain containing R. And we can prove that $\mathbb{Q}\left[\sqrt{2}\right]$ is a domain, so

$$\mathrm{Frac}\left(\mathbb{Q}\left[\sqrt{2}\right]\right) = \mathbb{Q}\left[\sqrt{2}\right].$$

Some of you use $\sqrt{3} \notin \mathbb{Q}\left[\sqrt{2}\right]$ to show $\mathbb{R} \neq \mathbb{Q}\left[\sqrt{2}\right]$ (however, need some computations). Some of you use $\mathbb{R}$ is uncountable but $\mathbb{Q}\left[\sqrt{2}\right]$ is countable. Both ways are great. (Note that $\mathbb{Q}\left[\sqrt{2}\right] \cong \mathbb{Q} \times \mathbb{Q}$ and this is why it is countable).

3.17(v)/3.19(ii)/3.22/3.23(i) To prove something is a field, we need to show it is a commutative ring firstly. We can avoid tedious routine check about the associativity and distributivity by considering the given ring as the subring of a (commutative) ring we already know. Since it inherits all such properties from the larger ring.

For example, we can treat F_4 in 3.19 as the subring of the matrices ring $M_2(k)$ over the field k (here we take $k = \mathbb{F}_2$). Note that the matrices ring does not satisfy the commutativity, so we have to verify this for F_4.

After showing F is a commutative ring, we need to show the following

- $0 \in F$ and $1 \in F$;
- closed under two operation (addition and multiplication)
- inverse of every element with respect to the addition exists in F
- inverse of every *non-zero* element with respect to the multiplication exists in F

It is just some standard procedure, which is the part of reason why algebra is not difficult to handle sometimes.

Canvas problem 4 Why we need to prove the multiplication is "well-defined" and what you need to prove concretely? Because we define the multiplication depending on the representatives of equivalence classes. And every equivalence class has not only one representative in general. But a "good" (make-sense/"well-defined") multiplication should not depend on the choice of representatives. For instance, $1+3$ and $2+2$ both means 4, so it is natural to hope that $(1+3)\times 7 = (2+2)\times 7$.